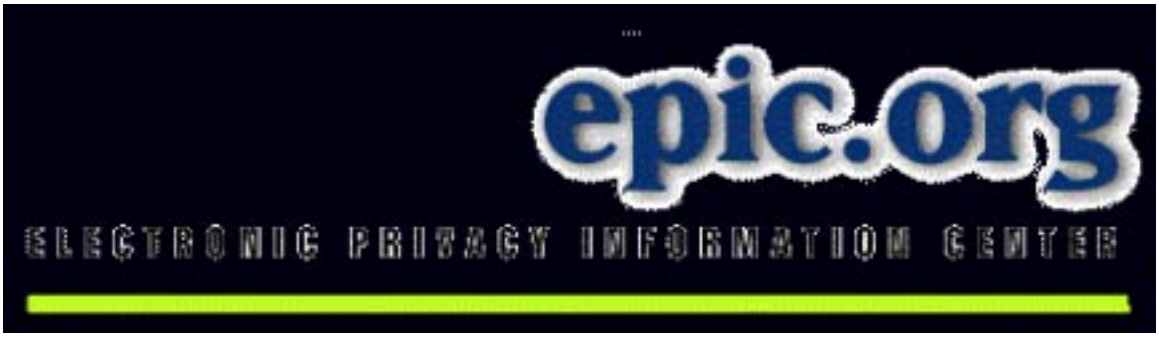

Testimony and Statement for the Record of

Marc Rotenberg, Director
Electronic Privacy Information Center

Hearing on
Financial Privacy and
The Financial Services Act of 1999

Before the

Subcommittee on Financial Institutions and Consumer Credit
Committee on Banking and Financial Services
U.S. House of Representatives

July 20, 1999
2218 Rayburn House Office Building

My name is Marc Rotenberg.[1] I am the Executive Director of the Electronic Privacy Information Center (EPIC) in Washington, DC.[2] I appreciate the opportunity to testify today before the Subcommittee on Financial Institutions and Consumer Credit regarding financial privacy and H.R. 10, The Financial Services Act of 1999.

Financial privacy is a critical concern for American consumers. The rise of new financial institutions, new financial practices, and new banking regulations, has also caused growing public concern over the privacy of personal information and the risk of disclosure of private financial data. More than a quarter of a million Americans opposed a banking regulation that would have established extensive government reporting requirements on routine financial transactions. And polls routinely show that the lack of privacy protection is contributing to growing public unease about the use of the Internet for commercial transactions.

It is therefore important that the Subcommittee on Financial Institutions continues to look closely at issues concerning financial privacy. Consumer confidence is critical to the stability of the financial system and the development of new commercial services. Without real safeguards for private personal information, the consumer expectation of privacy in routine financial transactions will be severely undermined.

In the statement below, I have answered the various questions put forward by the Subcommittee. In some sections, I have described broadly some of the recent developments that may help the Members understand the problem of privacy protection in a larger context. These include the development of new marketing practices, the impact of the EU Data Directive, and the relationship between federal and state privacy laws.

In other sections, I have described in more detail specific problems with the privacy provisions in H.R. 10, including Title V and section 351 on medical record confidentiality. These sections contain specific recommendations for how the bill could be changed to better protect the private information of American consumers.

In summary, there will be significant benefits to consumers in the rise of new financial services and products. But until strong privacy safeguards are established, the process of financial modernization will remain unfinished.

---

[1] Executive director, Electronic Privacy Information Center; adjunct professor, Georgetown University Law Center; editor, *The Privacy Law Sourcebook 1999: United States Law, International Law, and Recent Development;* editor (with Philip Agre) *Technology and Privacy: The New Landscape* (MIT Press 1998).

[2] The Electronic Privacy Information Center is a project of the Fund for Constitutional Government, a non-profit charitable organization established in 1974 to protect civil liberties and constitutional rights. More information about EPIC is available at the EPIC web site http://www.epic.org.

QUESTIONS POSED

1. Significant debate is occurring over whether financial institutions should be allowed to share customer information with their affiliates and nonaffiliated parties. Please comment on the benefits of information sharing and whether you believe additional protections are needed under the Fair Credit Reporting Act or other laws.

First, the concept of "affiliate sharing" is very much at odds with traditional privacy protection. Simply stated, privacy protection is the ability of individuals to limit the use of their personal information for a particular purpose. When, for example, a patient gives information to a doctor regarding a medical condition so that the doctor can provide a comprehensive diagnosis, there is a clear understanding that personal information will not be used for unrelated purposes, and if it is shared with a third party, it is only for purposes necessary to render the service provided.

Affiliate sharing transfers control over personal information from consumers to a corporate entity that may be engaged in a wide range of business practices unrelated to the specific purpose for which the information was provided. If a customer provides financial information to a bank for the purpose of getting a home loan and that information is subsequently used by an affiliated insurance company to provide information about insurance products, then it is clear that the customer's expectation of privacy when he or she provided that information to obtain a home loan was violated. As Justice Thurgood Marshall once wrote, "Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[3]

Second, the growth of the Internet and the rise of electronic commerce are leading many businesses to rethink their business models. I think it should also encourage more careful consideration of innovative privacy approaches and whether it is really necessary to collect so much personal information for a business to succeed in the age of the Internet. On the one hand, Internet-based businesses create new and unique privacy risks. It is much easier to track and profile customers on-line than it is in the physical world. If you grab a brochure in a bank for an IRA or clip out an ad in a newspaper for a home equity loan, those facts are still private information until you actually contact the bank or the lender. In the on-line world, if you download an ad for the same IRA or click on an ad for that same home equity loan, chances are good that some record will be created of your interest in these financial products.

At the same time, there are many ways to do business online that require the collection of less personal information and actually reduce privacy risks. It has become so

[3] *Smith v. Maryland*, 442 U.S. 735, 749 (1979)(Marshall, J., dissenting).

easy to set up an electronic storefront on the World Wide Web that many of the costs associated with brick and mortar businesses have literally disappeared. Marketing is cheaper and more efficient. Information is much more widely available to consumers.

The bottom-line is that access to personal information held by affiliated parties is not needed for a company to be profitable or to provide services to customers. Individuals should retain the ability to decide for themselves how personal information is to be used. That is the basis of privacy protection.

2. If you believe that additional financial privacy protections are necessary, please describe how new government mandates can be balanced with the information flow that is necessary to conduct daily business operations. In particular, discuss how the additional privacy protections you propose would affect credit availability and the ability of institutions to offer consumers lower cost products.

While the relationship between privacy and the free flow of information is oftentimes described as a "balance" or a "trade-off," it is important to understand that there are many instances where privacy protection is necessary to ensure the free flow of information. Consider how valuable the telephone system or the mail service is for the daily exchange of information on everything from confidential business plans to medical record to private messages among friends and family. It is precisely because privacy is provided in these network environments that businesspeople are willing to place valuable commercial documents in a paper envelope or people feel free to tell their most intimate secrets into a device that connects millions of users across the country.

Similar issues arise with the disclosure of personal information to financial institutions. If customers cannot be assured that their personal information will not be improperly disclosed, then they may be less willing to provide information and to take advantage of new commercial services. Privacy protection is clearly an essential element of establishing trust and confidence in the online world.

I cannot specifically assess how new privacy rules would affect credit availability or the ability of institutions to offer consumer lower cost products, but I will make two observations. First, credit markets in the United States seem to operate fairly well even with government regulation and government oversight. Second, the price competition that is developing on the Internet today, which has enabled consumers to find many products at much lower costs than they could previously, seems to have very little to do with the sharing of personal information. Instead price competition has resulted from much better access to price information that has made consumers more knowledgeable and markets more efficient. I think it would be a mistake to assume that lower prices for consumers requires extensive collection and use of personal information.

3. Please provide comments specifically addressing the privacy provisions in H.R. 10 as passed by the House. In particular, please discuss the exceptions that are in the bill and whether they are sufficient to permit typical, everyday business transactions to continue.

Comments on TITLE V- PRIVACY; Subtitle A - Disclosure of Nonpublic Personal Information

H.R. 10 fails to adequately protect consumer privacy in a variety of ways:

- There is no limitation on use of publicly available information.
- There is no control whatsoever over disclosure to institution affiliates
- There is no opt-out for disclosure to an institution's marketing partners
- There is no notice to consumers of particular uses of information, undermining the utility of opt-out measures
- There is no requirement of convenient opt-out procedures
- There is no consumer access and verification of institution-held information

Overall, H.R. 10 keeps consumers in the dark about the dissemination and use of even their most personal financial data. It allows unfair information practices on the part of financial institutions, including confusing privacy policies, burdensome opt-out procedures, and abuse of the Act's wide range of exceptions

For example, the Act regulates disclosure of "personally identifiable financial information—(i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or the service performed for the consumer; or (iii) otherwise obtained by the financial institution."[4] Nonpublic personal information also includes "any list, description, or other grouping of consumers" assembled using private information held by the financial institution (e.g., a listing of the names and addresses of all account holders whose daily balance exceeds $1M). [5]

Unfortunately, the Act leaves the definition of publicly available information, which is not covered, to individual administrative agencies. This makes it impossible to determine which information categories fall under the Act's provisions. Nonetheless, one can reasonably expect names, addresses, and listed telephone numbers to be deemed publicly available. Instead of allowing financial institutions to continue providing the direct marketing industry with up-to-date mailing lists, the Act should limit disclosure of all personally identifying information. Currently, financial institutions may sell this information without customer notice or consent. At the very least, the Act should require adequate notice of all disclosures, even those involving publicly available information.

The Act also regulates disclosure of personal information only to nonaffiliates of the financial institution.[6] Thus, "any company that controls, is controlled by, or is under common control with another company" may freely receive account numbers, spending habits, and other sensitive information.[7] Consumers must have the opportunity to opt-out of disclosures to all third parties, excepting those who perform specific servicing or processing functions related to a consumer's account (e.g., printing checks). While section 502(e)(1) attempts to implement an exception of this type, the definition of necessary services, section 509(7), is overly broad. In particular, section 509(7)(C)

[4] § 509(4)(A).
[5] § 509(4)(C).
[6] § 502(a).
[7] § 509(6).

allows insurance companies to obtain private information for such nebulous purposes as "account administration." This language should be tightened to allow free access to consumer personal information only by third parties directly involved in the maintenance of the consumer's account.

The Act's most salient feature is its litany of exceptions to the notice and opt-out provisions. First, even unaffiliated third parties may obtain sensitive information "to perform services or functions on behalf of the financial institution, including marketing of the financial institution's own products or services or financial products or services offered pursuant to joint agreements between two or more financial institutions."[8] This clause allows marketing companies to continue compiling highly specific consumer profiles without the consumer's consent. The compilation of such profiles would likely qualify as a "service or function" under this section. Other exceptions are equally troubling. § 502(e)(3) authorizes unrestricted disclosure of personal information "to protect the confidentiality or security of [a financial institution's] records pertaining to the consumer." It is unclear how a consumer's privacy interests are protected by free disclosure of spending habits and other personal information. Finally, the purposes served by § 502(e)(4)—access to financial record information for the purposes of rating and regulating the institution—do not require disclosure of personally identifiable information. A guarantor can do her job with account numbers and balances that are not tied to particular individuals.

Disclosure to third parties that do not fall into one of the Act's many exceptions need only be preceded by notice and an opportunity for consumers to block disclosure.[9] The Act requires a statement of an institution's privacy policies and practices "at the time of establishing the customer relationship with the consumer and not less than annually."[10] The policy must include the "categories of persons to whom the information is or may be disclosed." § 503(b)(1)(A). However, since this category is limited to nonaffiliated third parties (even those that perform marketing services for the institution), institutions are likely to include this uninformative phrase in their privacy statements. A consumer will not know what to make of a phrase like "nonaffiliated third party," yet such a disclosure, without more, would appear to satisfy an institution's duties under the Act. Furthermore, there is no provision for disclosure of particular uses of a consumer's personal information. Language requiring a clear explanation of who will receive personal information, and what will be done with it, should be added.

Finally, as noted above, consumers should be informed of an institution's disclosure policies regarding publicly available information as well nonpublic data categories. The opt-out requirement applies only to unaffiliated third parties who are not

[8] § 502(b)(2).
[9] § 502(a)-(b).
[10] § 503(a).

included in the marketing exception described above.[11] Thus, consumers are powerless to prevent widespread dissemination of their personal information to marketing firms as well as any institutions that have entered joint agreements with a consumer's institution. This result is inconsistent with the fundamental privacy principle of individual control over dissemination and use of personal information. Consequently, the Act should at least allow consumers to opt-out of any disclosure of personally identifiable data. Enacting an "opt-in" procedure would further the goals of information privacy even more. By making non-disclosure the default, an opt-in system gives individuals true control over their personal information. Because the data in question is so personal—purchase information, account numbers, and so on—an opt-in procedure should be implemented. In the alternative, the Act should at least specify that nondisclosure options be reasonably convenient for the consumer to exercise. As written, the Act requires only "an explanation of how the consumer can exercise" an opportunity "to direct that such information not be disclosed."[12] Thus financial institutions can create burdensome opt-out conditions in hopes of reducing the number of customers exercising the option. This is clearly incompatible with the Act's privacy protection objective. Consequently, the Act should require convenient opt-out procedures.

Finally, the Act includes no language ensuring consumers an opportunity to access and verify personal information after collection. A robust access and update system benefits both consumers and institutions. Allowing individuals to check the relevance of personal data held by financial institutions will foster a sense of empowerment among consumers, who will disclose information more readily knowing that they can verify it later. Along with the benefits of increased consumer trust, institutions stand to gain up-to-date personal information provided by the consumers themselves. Access and verification rights shift some of an institution's updating costs to the consumer. For these reasons, the Act should require access and correction procedures.

Comments on TITLE III; Subtitle E - Confidentiality; Sec. 351, Confidentiality of Health and Medical Information

One of the biggest privacy issues that the country faces today is the protection of medical record information, and both the Senate and the House are actively working to adopt legislation to protect the medical records of Americans. Section 351 of the Financial Services Act of 1999 attempts to address the medical privacy issue by limiting the disclosure of certain medical information. However well intended the privacy provision may be, it is likely to cause more problems than it solves.[13] It will almost certainly reduce the level of privacy protection for medical records that most Americans

[11] § 502(b)(2).
[12] § 502(b)(1)(B)-(C).
[13] "Still Not Private Enough," *The Washington Post*, July 8, 1999 at A24.

currently enjoy under state law or are likely to receive under either guidelines developed by the Secretary of HHS or medical privacy legislation passed by Congress.

Section 351 is a privacy provision only to the extent that it attempts to limit the disclosure of certain personal information. It does not contain the other elements of Fair Information Practices, including most significantly the right to obtain access to one's own medical record. This right is currently recognized in at least 34 states. Second, the exceptions in Section 351 are extremely broad. Law enforcement agencies could gain access to sensitive medical records upon a showing of far less information than is required to obtain a warrant.[14] Third, section 351 could effectively preempt state medical privacy provisions that are stronger than the language in the Financial Services Act.

The National Coalition for Patients' Rights has produced a useful paper "Protecting the Privacy of Medical Records: An Ethical Analysis" that provides an excellent basis for developing medical privacy legislation.[15] The recommendations outline the need to address such issues as record confidentiality, patient access, disclosure limitations, third party payers, psychotherapy, biomedical research, health services research, clinical research, law enforcement access and other topics.[16] The Model State Public Health Privacy Project, an effort currently underway at Georgetown University, has also developed a very good model statute for privacy protection.[17] Finally, there are the recent recommendations of the Health Privacy Working Group that are also worth close attention.[18]

I strongly urge you to either drop section 351 in the meeting of the conference committee or to adopt much stronger language in line with the National CPR proposal, the MSPHPP undertaking, and the PHPP Best Principles approach. There is clearly widespread support for strong medial privacy protection. I am sure that Americans do not want sensitive medical records to be freely shared between banks, insurers, and securities dealers

4. Currently consumers are afforded privacy protection under a combination of Federal and State laws. With respect to financial privacy, how do federal and state laws complement, reinforce, or overlap one another?

Currently financial privacy laws provided an incomplete framework for protection. For example, there is no comprehensive protection for insurance records, while there is better protection for credit reports.

---

[14] In "compliance with a . . . investigation . . ." Sec. 351(a)(3)(E).
[15] http://www.nationalcpr.org/WP-request.html

[17] http://www.critpath.org/msphpa/privacy.htm. cited in *Privacy Law Sourcebook* 542.
[18] "Best Principles for Health Privacy," [http://www.healthprivacy.org/latest/Best_Principles_Report.pdf].

Some states have moved quickly to address public concerns about financial privacy, while others have moved more slowly. Enforcement of current law is oftentimes uneven, though a prosecution can have a significant impact across an entire industry

In general the best approach to privacy protection is for the Congress to establish minimum standards for state regulatory schemes. For example, the Video Privacy protection Act of 1988 states simply "The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section."[19] In this manner, the exercise of federal authority to protect privacy still allows that states to function as "laboratories of democracy."[20]

The Financial Services Act should be make similar allowances for state regulatory authorities to develop new safeguards and new privacy protection as circumstances require.

5. Please discuss any concerns you may have about the Federal and State governments collecting and disseminating consumer information. For instance, it appears that State divisions of motor vehicles routinely provides vehicle registration information to commercial entities. In addition, last year IRS employees were found to have been "snooping" into neighbor and other people's files. Should consumers have the right to "opt out" of the government sharing information? Please discuss what changes, if any, you would recommend with respect to Federal and State government privacy policies and practices.

Consumers who provide information to a federal or state agency to obtain a service, receive a benefit, or comply with a legal obligation, have little choice when asked to provide personal information.

In the past week my organization filed a brief in the Supreme Court in the case concerning the Drivers Privacy Protection Act of 1994 because we believe that there are significant privacy interests in the collection and use of personal data maintained by state agencies.[21] Under the DPPA states are regulated only to the extent that they choose to take personal information provided to a state agency for the purpose of a obtaining a license to operate a motor vehicle on a public roadway and then subsequently sell or disclose that information to purposes unrelated to the operation of the Department of Motor Vehicle or the protection of public safety. We recommended to the Court that the DPPA be upheld over the objection that some of the states have made on federalism grounds.

---

[19] 18 U.S.C. § 2710(f) cited in *Privacy Law Sourcebook* 139.

[20] New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

[21] Brief Amicus Curiae of the Electronic Privacy Information Center in Support of Petitioners, Reno v. Condon, U.S. Supreme Court, No. 98-1464 (filed July 15, 1999). [http://www.epic.org/privacy/drivers/epic_dppa_brief.pdf]

More generally we support the establishment of rights based on the Privacy Act of 1974 that give individuals greater control over their information that is collected and used by federal and state agencies.

6. The government agencies all have websites. These websites contain privacy policies. Are the policies "clearly and conspicuously disclosed" to consumers? Some of the agencies collect information, while others do not. Some use "cookies," while others do not. Should the privacy policies, collection of information and use of cookies by the government be consistent?

I have no specific information about whether the privacy policies at government websites are "clearly and conspicuously disclosed" to consumers. However, EPIC did conduct the first comprehensive survey of web site privacy policies back in 1997. We reviewed 100 of the most frequently visited web sites on the Internet.[22] We checked whether sites collected personal information, had established privacy policies, made use of cookies, and allowed people to visit without disclosing their actual identity.

We found that about half of the sites that we surveyed in 1997 collected personal information. This was typically done for on-line registrations, surveys, user profiles, and order fulfillment. We also found that few web sites had explicit privacy policies (only 17 of our sample) and none of the top 100 web sites met basic standards for privacy protection. We also noted that users were unable to exercise any meaningful control over the use of cookies. However, we noted that anonymity played an important role in online privacy, with many sites allowing users to access web services without disclosing personal data. We said that:

> Users of web-based services and operators of web-based services have a common interest in promoting good privacy practices. Strong privacy standards provide assurance that personal information will not be misused, and should encourage the development of on-line commerce. We also believe it is matter of basic fairness to inform web users when personal information is being collected and how it will be used.

We recommended that:

- Web sites should make available a privacy policy that is easy to find. Ideally the policy should be accessible from the home page by looking for the word "privacy."
- Privacy policies should state clearly how and when personal information is collected.

[22] EPIC, "Surfer Beware I: Personal Privacy and the Internet" (1997) [http://www.epic.org/reports/surfer-beware.html]

- Web sites should make it possible for individuals to get access to their own data
- Cookies transactions should be more transparent
- Web sites should continue to support anonymous access for Internet users.

In 1998 the FTC conducted its own survey of privacy policies. Although the survey looked at more web sites, the FTC survey was in some critical respects narrower than the original EPIC survey.[23] The FTC focused on the number of web sites that collect personal information and also on the number of web sites that had a privacy policy. But the FTC largely ignored the crucial role of anonymity in privacy protection. The FTC also lowered the bar by defining Fair Information Practices to be simply "notice," "choice," "access" and "security." [24] Although we did not look at the full range of Fair Information Practices in 1997, we followed the OECD practice in inquiring whether there were "use limitations" or "secondary use restrictions" in the privacy policies we found. This point is important because much of privacy law turns on the principle of finality – the principle that information is collected for a particular purpose and that information should be used only for that purpose unless meaningful consent is obtained from the data subject.

In 1998 we undertook a second survey to determine whether industry was doing a good job encouraging its own members to adopt privacy policies. "Surfer Beware II: Notice is Not Enough" surveyed the privacy policies of 76 new members of the Direct Marketing Association (DMA).[25] We chose the DMA because it has been a leading proponent of self-regulation and because it has undertaken a number of efforts to encourage privacy protection through self-regulation. These included a policy announced in October 1997 that the DMA would require future members to post a privacy policy and provide an opt-out capability. Of the 76 new members we examined, only 40 had Web sites and of these, only eight sites had any form of privacy policy. We examined these policies and found that only three of the new members have privacy policies that satisfied the DMA's requirements set out in October 1997. None of the sites examined allowed individuals to gain access to their own information. We concluded that the DMA's efforts to promote privacy practices is having little impact on its new members, even after repeated assurances from the DMA that this approach is effective.

There should be comprehensive federal guidelines for government web sites and theses guidelines should reflect the principles of the Privacy Act of 1974. Individuals should be able to determine whether there are records held in an agency that contain information concerning that individual. And people should have the ability to gain access to personal information about them held by federal agencies. Simply posting a notice is not enough to ensure that the principles of the Privacy Act are upheld.

On the topic of cookies, it is important to distinguish between cookies that collect personal identifiable information and those that do not. A cookie that is tied to a known

---

[23] FTC, "Online Privacy: A Report to Congress" (1998) [http://www.ftc.gov/reports/privacy3/index.htm].

[24] Prepared statement of the Federal Trade Commission on "Internet Privacy" before the Subcommittee on Courts and Intellectual Property of the House Judiciary Committee, March 26, 1998 [http://www.ftc.gov/os/1998/9803/privacy.htm

[25] [http://www.epic.org/reports/surfer-beware2.html]

user raises significant privacy issues. Although any collection of personal information presents a privacy risk, the risk is more serious with cookies because the collection of the identifying data is often surreptitious, and lacking any reasonable means for individuals to exercise control over the collection and use of data. Thus a cookie policy for the federal government should begin by noting whether personal identifiable information is collected from the person visiting the web site.

Finally, in this discussion of website policies for Federal and State governments, I would add that everything should be done to ensure that individuals are able to access information from government agencies anonymously, i.e. without being required to disclose one's identity. A person who goes to the IRS web site, for example, to download a form or publication should be able to do so without any concern that a record will be created of that inquiry. Of course consumers should remain free to disclose personal information when it may be beneficial to receive some additional service or information. But federal and state governments would stay on the right track if they kept in mind the value of providing information to consumers without requiring the collection of personally identifiable information. This is far more important than whether a privacy policy is clear and conspicuous.

7. Please identify and discuss your group's privacy policy. Is your privacy policy clearly and conspicuously disclosed to members and supporters of your group? Does your group rent, sell or lease its membership list to third parties? Are your members and supporters given the opportunity to "opt out" of information sharing with third parties?

The EPIC Privacy Policy is displayed on our homepage.[26] It states simply:

> **EPIC Mailing List**
>
> If you are interested in receiving the EPIC Alert, we ask for your email address so that we can send it to you. You can also receive the EPIC Alert by visiting the EPIC Alert archive at our web site. The EPIC Alert mailing list is used only to mail the EPIC Alert and to send notices about EPIC activities. We do not sell, rent or share our mailing list. We also intend to challenge any subpoena or other legal process seeking access to our mailing list. We do not enhance (link to other databases) our mailing list or require your actual name.
>
> **EPIC Web Site**

[26] "EPIC Privacy Policy," http://www.epic.org/epic/privacy_policy.html.

> We do not enable cookies and we do not collect personally identifiable information at our web site. We periodically delete usage logs.
>
> **EPIC and Amazon**
>
> We are an Amazon Associate and sell books at the EPIC Bookstore on topics that we think will interest our users. Amazon will ask you for certain personal information, such as mailing address and credit card number, to fulfill your order. Amazon also has a privacy policy and does not sell or rent information about its customers. EPIC does not receive any personally identifiable information about EPIC Bookstore customers from Amazon.

Another web site that we manage – privacy.org – has a simple but direct privacy policy:[27]

> The Privacy Page collects no personally identifiable information, maintains no mailing list, and does not put cookies (or anything else) on your hard disk. We are an information resource, not an information sponge.
>
> Have a nice day.

As I indicated, privacy protection is more about practices than policies. A very large notice that says "We collect your personal information and toss it in the street" provides much less protection than an actual set of procedures that reflects a substantive commitment to privacy protection.

For example, we believe that mailing lists should be operated on an opt-in basis and that it should be as easy to get off a list as it is to get on a list. It is as easy to unsubscribe to the EPIC Alert as it is to subscribe to it.[28] Every EPIC Alert that we send out includes instructions at the end for unsubscribing. And we have built a mailing of over 10,000 subscribers to the EPIC Alert who have opted-in. We have always avoided the practice of merging lists or adding people to our list without their actual consent.

We recognize also that there are some people who may like to get information without subscribing to a mailing list. So all the information that is sent out in the EPIC Alert is also available at our web site and it can be viewed anonymously, without any requirements that personal information be disclosed.

Now some may say that as a privacy organization we have to be particularly sensitive to privacy concerns and so it is understandable that we would have a very good privacy policy, and I think that is true. But it is also true that we understand that privacy

[27] "The Privacy Policy of Privacy.org," http://www.privacy.org/privacy_policy.html.
[28] "Subscribing to the EPIC Alert," http://www.epic.org/alert/subscription.html.

protection is not just about what you say you'll do with personal information; it's about what you actually do. It's about procedures and practices, and not just the words on a web site.

It's also important to note that for many years, a very high level of privacy protection characterized the Internet, at least in terms of data collection practices. There were few incentives to collect and use personal information. People could routinely access web sites without disclosing their actual identity and mailing lists all observed the convention of opt-in, It is only recently that we are beginning to see the rapid increase in the collection of personal information. Privacy policies are doing little to slow that process.

8. In the United States, privacy laws are designed largely on an industry basis while many other countries have one comprehensive privacy statute. Given the fundamental difference between U.S. privacy laws and other countries, what effect will compliance with the EU Directive have on U.S. commerce abroad?

I believe the E.U. Directive has already had several very positive effects on U.S. commerce abroad. First, it has simplified the process of doing business in Europe. Prior to adoption of the E.U. Data Directive, European countries operated with many different privacy laws that made it difficult not only to conduct trade within Europe but also for U.S. firms operating in Europe to comply with the laws of the various countries. Large, established firms such as Citibank and American Express had the resources and the incentives to develop close ties to privacy agencies and to develop practices that complied with national law. But for most small and medium sized firms the obstacles were great.

With the adoption of the E.U Data Directive, European countries sought to promote trade within Europe and to remove the barriers to the free flow of good and services, labor and capitol. The Directive has helped firms outside of Europe develop policies and practices that will now be acceptable across the European Union. There is now a single reference document that covers virtually all of the privacy obligations for financial firms operating in Europe. I suspect this is a simpler regulatory approach than the one faced by foreign firms operating in the United States.

Second, the EU Data Directive also led to the creation of institutions that have focused on the problem of how to protect privacy in the years. The Working Group, established by Article 29 of the Directive, has been the source of some of the most significant proposals and policy recommendation of any government entity in the world. The Article 29 working group has tackled such issues as anonymity, cookies, and self-regulation in an even-handed manner

The United States would have benefited greatly over the last several years if there were a similar agency with the expertise and authority to provide guidance and recommendation in this critical area of public policy.

The third significant advantage of compliance with the EU Data Directive is that it has forced a raising of privacy protection in the United States by focusing on the central question of whether we really have adequate privacy protection in this country. The EU Data Directive is not so much a problem as it is a reminder that our privacy laws are out of date and that there is much work to be done in this country to ensure the protection of this essential freedom. Further action against the EU Data Directive will not make the privacy concerns in the United States go away. In the end, we need stronger privacy safeguards not to satisfy European government, but to assure the protection of our own citizens.[29]

9. Commerce taking place over the Internet is largely subject to a variety of industry self-regulatory efforts. Do you believe that self-regulation is sufficient at the present time, or are new government mandates warranted?

I believe that the current efforts to promote industry self-regulation will not adequately address the public concerns about privacy and the Internet. Industry policies are typically incomplete, incoherent, and unenforceable. They are having little impact on actual data collection practices. Instead of reducing the demand for personal information or encouraging the development of privacy enhancing techniques, industry privacy policies are literally papering over the growing problem of privacy protection online.

A better approach would be to establish a legal framework that provides simple, predictable, uniform rules to regulate the collection and use of personal information. Not only is this approach consistent with US privacy legislation, it would also provide clarity and promote trust for consumers and businesses in the new online environment. I also believe that protecting privacy rights in law would encourage the development of better techniques to protect privacy and, in the long term, reduce the need for government intervention. The key to effective privacy legislation is to pursue the enforcement of Fair Information Practices and the development of methods that reduce the need for personally identifiable information.

Up until a few years ago, legislating privacy protection was a straightforward problem. The basic goal was to outline the responsibilities of organizations that collect personal information and the rights of individuals that give up personal information.

---

[29] Testimony and Statement for the Record of Marc Rotenberg Director, Electronic Privacy Information Center Adjunct Professor, Georgetown University Law Center on The European Union Data Directive and Privacy Before the Committee on International Relations, U.S. House of Representatives May 7, 1998 [http://www.epic.org/privacy/intl/rotenberg-eu-testimony-598.html]. See also Rotenberg, *The Privacy Law Sourcebook* 505-29 ("Materials on 'Safe Harbor' Proposal").

These rights and responsibilities are called "Fair Information Practices" and they help ensure that personal information is not used in ways that are inconsistent with the purpose for which it was collected. Fair Information Practices typically include the right to limit the collection and use of personal data, the right to inspect and correct information, a means of enforcement, and some redress for individuals whose information is subject to misuse.[30]

Fair Information Practices are in operation in laws that regulate many sectors of the US economy, from companies that grant credit to those that provide cable television services.[31] Your video rental store is subject to Fair Information Practices as are public libraries in most states in the country. The federal government is subject to the most sweeping set of Fair Information Practices. The Privacy Act of 1974 gives citizens basic rights in the collection and use of information held by federal agencies. It also imposes on these same agencies certain obligations not to misuse or improperly disclose personal data.[32]

Not only have Fair Information Practices played a significant role in framing privacy laws in the United States, these basic principles have also contributed to the development of privacy laws around the world and even to the development of important international guidelines for privacy protection. The most well known of these international guidelines are the OECD Recommendations Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.[33] The OECD Privacy Guidelines set out eight principles for data protection that are still the benchmark for assessing privacy policy and legislation.[34] These are:

---

[30] See generally, Robert Gellman, "Does Privacy Law Work?" in P. Agre and M. Rotenberg, *Technology and Privacy: The New Landscape* (MIT Press 1998)

[31] *Privacy Law Sourcebook* 1-37, 100-02 (Fair Credit Reporting Act of 1970, Cable Communications Policy Act of 1984).]

[32] *Privacy Law Sourcebook* 38-56.

[33] *Privacy Law Sourcebook* 179-205.

[34] BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: (a) with the consent of the data subject; or (b) by the authority of law.

Security Safeguards Principle. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Individual Participation
- Accountability

The United States and more than a hundred US companies pledged to support the OECD Guidelines almost twenty years ago. It is worth noting also that the United States has a particularly strong tradition of extending privacy rights to new forms of technology. For example, subscriber privacy provisions were included in the Cable Act of 1984. New protections for electronic mail were adopted in the Electronic Communications Privacy Act of 1986.[35] Video rental records were safeguarded as a result of the Video Privacy Protection Act of 1988.[36] And auto-dialers and junk faxes were regulated by the Telephone Consumer Protection Act of 1991.[37] Even the original Privacy Act of 1974 came about in response to growing public concern about the automation of personal records held by federal agencies.

Viewed against this background, the problem of privacy protection in the United States in the early 1990s was fairly well understood. The coverage of US law was uneven: Fair Information Practices were in force in some sectors and not others. There was inadequate enforcement and oversight. Technology continued to outpace the law. And the Europeans were moving forward with a comprehensive legal framework to safeguard privacy rights of their citizens.

Unfortunately, just at the point in time when there was need for leadership in government to promote a privacy policy based on extending Fair Information Practices,

---

Individual Participation Principle. An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
Accountability Principle. A data controller should be accountable for complying with measures which give effect to the principles stated above.
Privacy Law Sourcebook 181-82.
[35] *Privacy Law Sourcebook* 103-36.
[36] *Privacy Law Sourcebook* 137-39.
[37] *Privacy Law Sourcebook* 149-57.

the Administration and Congress turned away from well established legal standards and traditions and proposed instead a search for solutions based on industry self-regulation.

Some said that the interactive nature of the Internet made possible a new approach to privacy protection, one that focused on individuals exercising privacy "choice" or "preferences." But providing a range of choices for privacy policies turns out to be a very complicated process, and there is no guarantee that a person's privacy preferences on one day will be the same the next. In the rush to avoid a "one size fits all approach," those who focused on privacy choices may have discovered, paradoxically, that "many sizes fits none." In other words simple, predictable, uniform rules make it easier for individuals to exercise control over their personal information than an endless selection of choices that turn out to be meaningless.

Other industry approaches emphasized the easy online availability of privacy policies. But in practice, making use of a web site privacy policy turns out to be cumbersome and impractical, and almost the antithesis of the Internet's architecture. The very networked nature of the Internet that enables users to move freely from one site to the next discourages standards that vary from one site to the next. If a user will click past a site because a graphic takes too long to load, can we reasonably expect that same person to read through the fine print of a privacy policy? Both of these approaches, which are the outcome of pursuing the industry policy of self-regulation, have made it more difficult -- not easier -- for individuals to protect their privacy online.

An additional problem was created by the somewhat awkward role of the Federal Trade Commission. Because the United States lacks an agency with the expertise and competence to develop privacy policies, the FTC was cast in the role of de facto privacy agency. But the FTC did not itself have the authority to enforce Fair Information Practices or to promote the development of the various privacy enhancing techniques that were being pursued by other privacy agencies around the world.[38] The FTC relied instead on its Section 5 authority to investigate and prosecute fraudulent or deceptive trade practices.

The better approach would have been to look at the Internet and ask how could it make it easier to apply and enforce Fair Information Practices. For example, one of the hard problems in privacy protection is ensuring that individuals are able to access and correct information about themselves. In the paper world, the right of access is an elaborate and costly process for both businesses and consumers. Records must be copied and sent by mail. In the online world it is much easier to provide ready access to profile information. In fact many web sites today, from airline reservations to online banking, are making information that they have about their customers more readily available to their customers over the Internet. It is not "choice" that customers are exercising but rather "control" over their personal information held by others.

[38] See, e.g., EC Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, "Anonymity on the Internet" (1997) reprinted in *Privacy Law Sourcebook* 404-15.

The Internet is also offering interesting developments in the use of techniques for anonymity and pseudo-anonymity to protect online privacy. These techniques enable commercial transactions while minimizing or eliminating the collection of personal information. Such techniques avoid the need for privacy rules simply by avoiding the rights and responsibilities that result from the collection and use of personal data.

10. Please feel free to provide any additional comments you may have on these issues.

The key to privacy protection is to give the give consumers the ability to control personal information held by third parties, and where possible to limit or eliminate the collection of personally identifiable information. I believe the Internet offers enormous opportunities to develop innovative, effective means to protect online privacy, but these efforts will only succeed if the goal is well understood. Simply posting a privacy policy will not protect privacy. It may in fact have the exact opposite effect if the policy serves the purpose of disclaiming any reasonable privacy claim that the consumer might have otherwise pursued. Thus the adequacy of these policies becomes crucial and the need to make very clear in statute the essential elements of Fair Information Practices is critical. It is not enough to simply state that a financial institution has an "affirmative and continuing obligation to respect the privacy of its customers," – the nature of these obligations should be spelled out and made clear to both customer and financial institutions.[39] This was the approach taken in the Privacy Act of 1974, and that Act has done well over the years. Where problems arise, it is from absence of enforcement or an overly broad reading of certain exceptions. But the key to effective privacy legislation is the articulation of specific Fair Information practices that make clear the rights of individuals who give up personal information and the responsibilities of those organizations that collect personal information

It is also very important to pursue innovative solutions to privacy issues. There are so many ways today to market, advertise and sell products without collecting personal information. Just to give one example, as an Amazon Associates, EPIC receives some of its revenue from the sale of books related to privacy, and civil liberties on the Internet. The EPIC Online Bookstore has done very well and we recently became an Amazon Affiliate so that we could also sell our publications through Amazon. But what is most extraordinary about all of this is that we are able to sell books to customers at our web site without collecting any personal information. All of the data is collected by Amazon.

The study proposed in section 508 is a good idea, but a more extensive and far-reaching project would look at the many emerging opportunities to conduct online commerce by means of transactions that do not require the collection and use of personal information. This may be a good project for the National Research Council. And if a

[39] § 501(a) ("Protection of Nonpublic Personal Information").

good solution is found – if robust techniques for enabling online commerce while protecting the collection and use of personal information are discovered – it will greatly benefit consumers and financial institutions in the years ahead.

Finally, I hope you will reconsider limitations on the reporting requirements contained in the Bank Secrecy Act and the proposed rollback of the entire regulatory requirement. Many privacy problems can be avoided simply by reducing the collection and use of personal information. The Bank Secrecy Act is simply too broad, too burdensome, and too intrusive. Efforts to repeal the Act are certainly worth pursuing.